

00001160 8d eb 66 46 bf e2 2b 0e 13 f5 f5 93 95 9c 1f da  
00001161 89 63 e8 1b 8f cc d9 86 76 13 ad 4e 4d f4 63 cf  
00001162 99 61 01 05 96 85 89 04 3c 4f ad 0c 1b 5e 95  
00001163 61 0f a1 9e 99 5e d9 1d 4c 81 be 84 55 e5 92 8d  
00001164 fb 24 24 c2 b9 26 0d 02 22 9a 8a aa 76 2e 1c 8f  
00001165  
00001166  
00001167  
00001168  
00001169  
00001170  
00001210  
00001220  
\*  
00001240  
00001250  
00001260  
00001270  
00001280  
00001290  
000012a0  
000012b0  
000012c0  
000012d0  
000012e0  
000012f0  
00001300  
00001310  
00001320  
00001330  
00001340  
00001350  
00001360  
00001370  
00001380  
00001390  
000013a0  
000013b0  
000013c0  
000013d0  
000013e0  
000013f0  
00001400  
00001410  
00001420  
00001430  
00001440  
00001450  
00001460  
00001470  
00001480  
00001490  
000014a0  
000014b0  
000014c0  
000014d0  
000014e0  
000014f0  
00001500  
00001510  
00001520



00001160  
00001161  
00001162  
00001163  
00001164  
00001165  
00001166  
00001167  
00001168  
00001169  
00001170  
00001210  
00001220  
\*  
00001240  
00001250  
00001260  
00001270  
00001280  
00001290  
000012a0  
000012b0  
000012c0  
000012d0  
000012e0  
000012f0  
00001300  
00001310  
00001320  
00001330  
00001340  
00001350  
00001360  
00001370  
00001380  
00001390  
000013a0  
000013b0  
000013c0  
000013d0  
000013e0  
000013f0  
00001400  
00001410  
00001420  
00001430  
00001440  
00001450  
00001460  
00001470  
00001480  
00001490  
000014a0  
000014b0  
000014c0  
000014d0  
000014e0  
000014f0  
00001500  
00001510  
00001520

00001160  
00001161  
00001162  
00001163  
00001164  
00001165  
00001166  
00001167  
00001168  
00001169  
00001170  
00001210  
00001220  
\*  
00001240  
00001250  
00001260  
00001270  
00001280  
00001290  
000012a0  
000012b0  
000012c0  
000012d0  
000012e0  
000012f0  
00001300  
00001310  
00001320  
00001330  
00001340  
00001350  
00001360  
00001370  
00001380  
00001390  
000013a0  
000013b0  
000013c0  
000013d0  
000013e0  
000013f0  
00001400  
00001410  
00001420  
00001430  
00001440  
00001450  
00001460  
00001470  
00001480  
00001490  
000014a0  
000014b0  
000014c0  
000014d0  
000014e0  
000014f0  
00001500  
00001510  
00001520

# An OpenBTS GSM Replication Jail for Mobile Malware

Axelle Aprille

Virus Bulletin Conference, October 2011



**Thou Shalt Not Spread (Nor Leak)**



**Thou Shalt Not Spread (Nor Leak)**



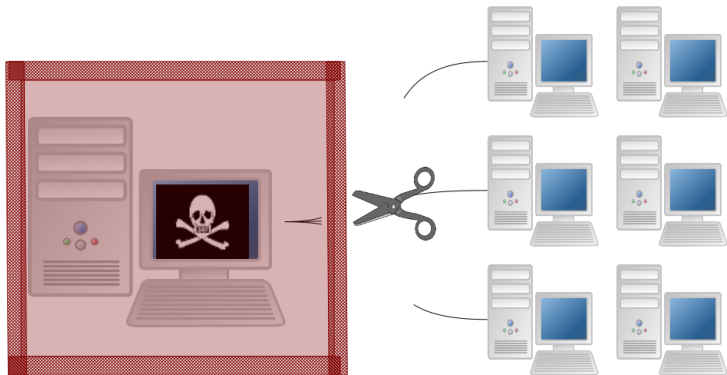
**Thou Shalt Not Spread (Nor Leak)**



**Thou Shalt Not Spread (Nor Leak)**



**Thou Shalt Not Spread (Nor Leak)**



**Thou Shalt Not Spread (Nor Leak)**



**Thou Shalt Not Spread (Nor Leak)**



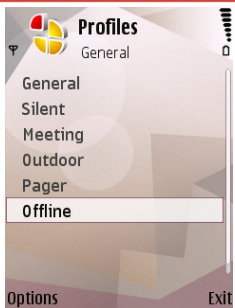


Thou Shalt Not Spread (Nor Leak)



**Thou Shalt Not Spread (Nor Leak)**

# Jail 1. Remove SIM/ Offline/ Flight mode



- ▶ Secure... probably
- ▶ Behaviour: changed!

Malware Name	Online	Offline
SymbOS/Album	Sends 2 SMS	-
SymbOS/Acallno	Trojan spyware	Can't be activated
SymbOS/Feixiang	Sends 2 SMS	Sends <b>1</b> SMS
Java/Konov, SymbOS/- ZoomSms	Sends SMS	System lag

## Jail 2. Use an emulator

- ▶ Good Android emulator, but other OS?
- ▶ Same behaviour change problem
- ▶ Hardware exploits/ VM detection



## Jail 3. Faraday cage



Not that easy to build...

## Jail 3. Faraday cage

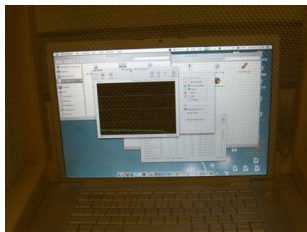


Not that easy to build...

- ▶ How to see the screen?

Courtesy of J. Daniels

<http://www.jeddaniels.com/2007/faraday-cage-part-1/>

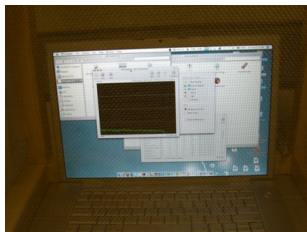


Not that easy to build...

- ▶ How to see the screen?
- ▶ Access to keyboard?

Courtesy of J. Daniels

<http://www.jeddaniels.com/2007/faraday-cage-part-1/>



Courtesy of J. Daniels  
<http://www.jeddaniels.com/2007/faraday-cage-part-1/>

### Not that easy to build...

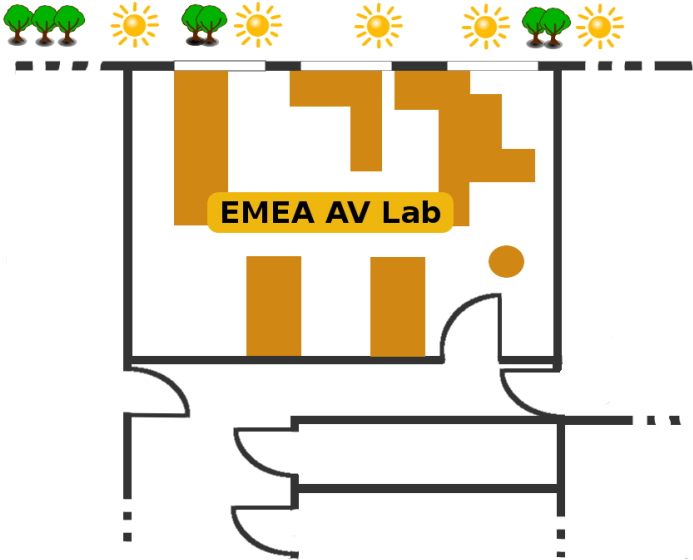
- ▶ How to see the screen?
- ▶ Access to keyboard?

### Large Faraday cages

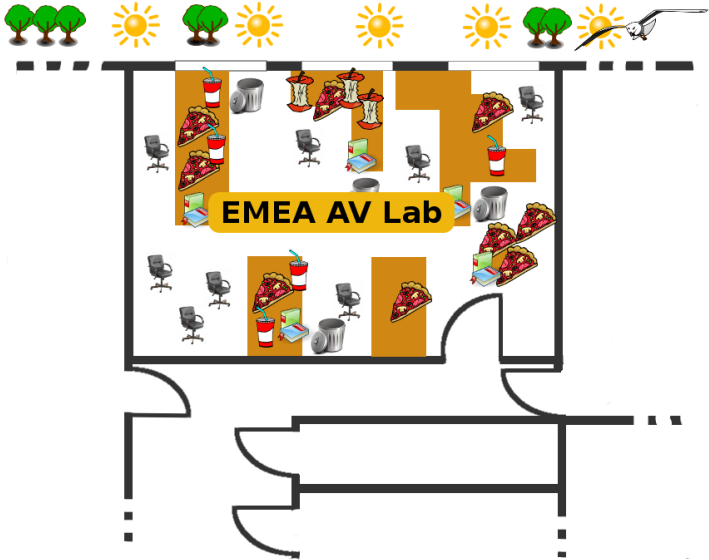
Expensive + Weight



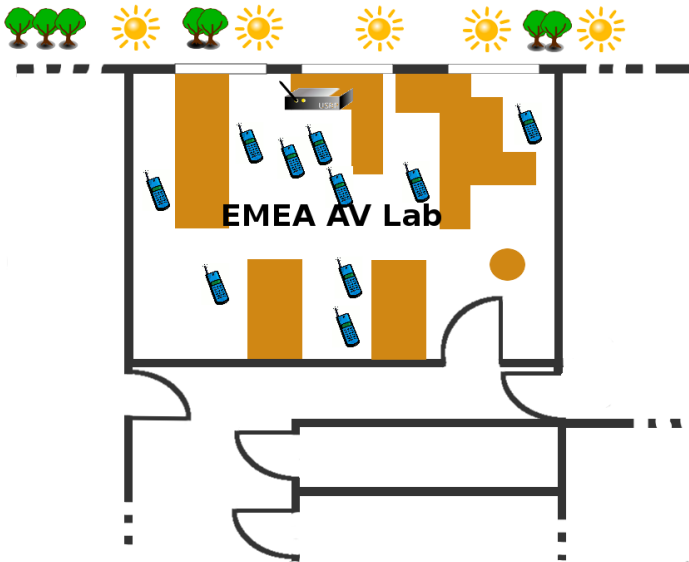
# Build your own operator network!



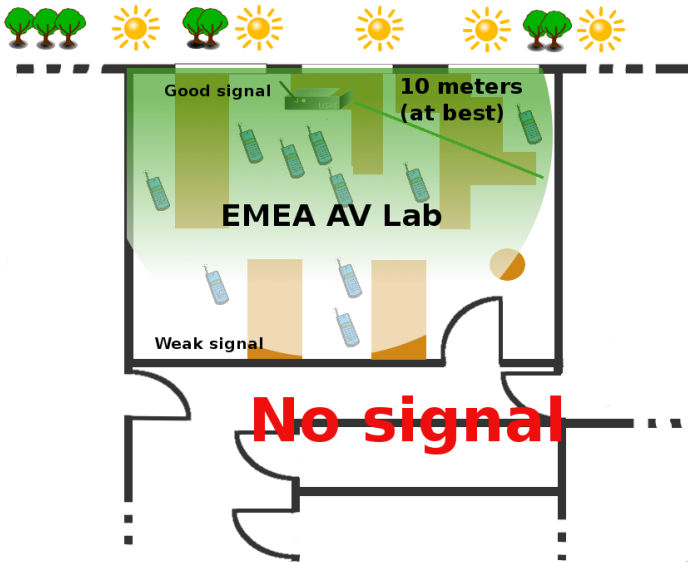
# Build your own operator network!



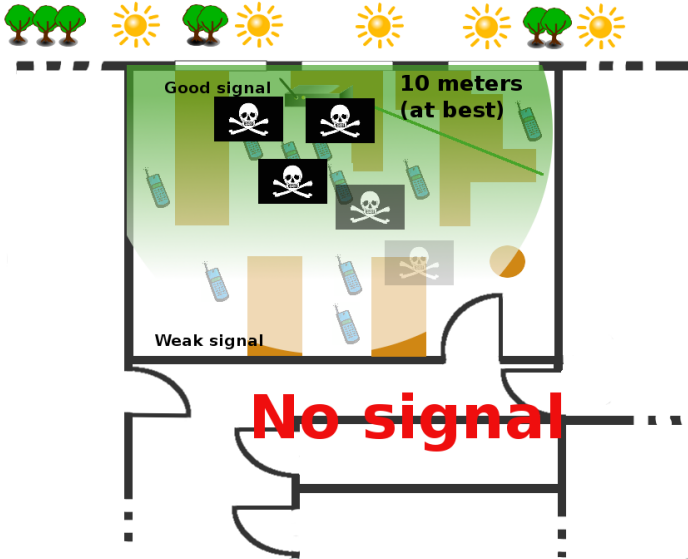
# Build your own operator network!



# Build your own operator network!



# Build your own operator network!



## OpenBTS

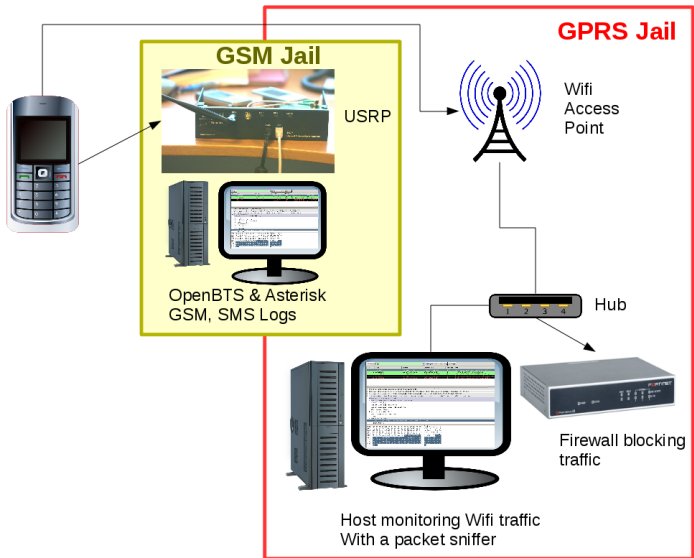
- ▶ Open source project
- ▶ Local GSM operator = USRP + accurate clock + host running OpenBTS / Asterix
- ▶ No GPRS, EDGE, UMTS...

OpenBTS is a registered trademark of Range Networks, Inc.

## And nanoBTS-OpenBSC?

Good (perhaps better?)... but 6 times more expensive

# Jail Architecture



**2103**



**Infected by  
Zitmo**

**2102**



**Attacker  
Intercepts SMS**

**2111**



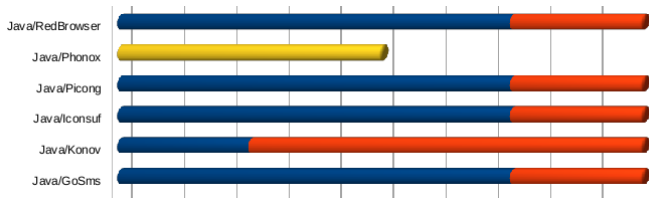
**Genuine  
Friend / Bank  
Sends SMS  
to infected**

What the analyst sees...

Part 1. ... when the phone is offline

Part 2. ... with an OpenBTS-based jail





Blue: offline, Red: with GSM jail, Yellow: +GPRS jail.  
Full results: see paper.

## Main Advantages

- ▶ Behaviour similar to real conditions
- ▶ See SMS contents and details
- ▶ No leak to real networks
- ▶ Low cost

## Limitations

- ▶ Sample requires a WCDMA bearer
- ▶ MMS not handled
- ▶ Dynamic analysis limitations

# Thank You !

Follow us on <http://blog.fortinet.com>  
or twitter: **@FortiGuardLabs**

Axelle Apvrille

aka *Crypto Girl*

/mobile malware reverse engineering/

aapvrille@fortinet.com



Slides edited with **LOBSTER**